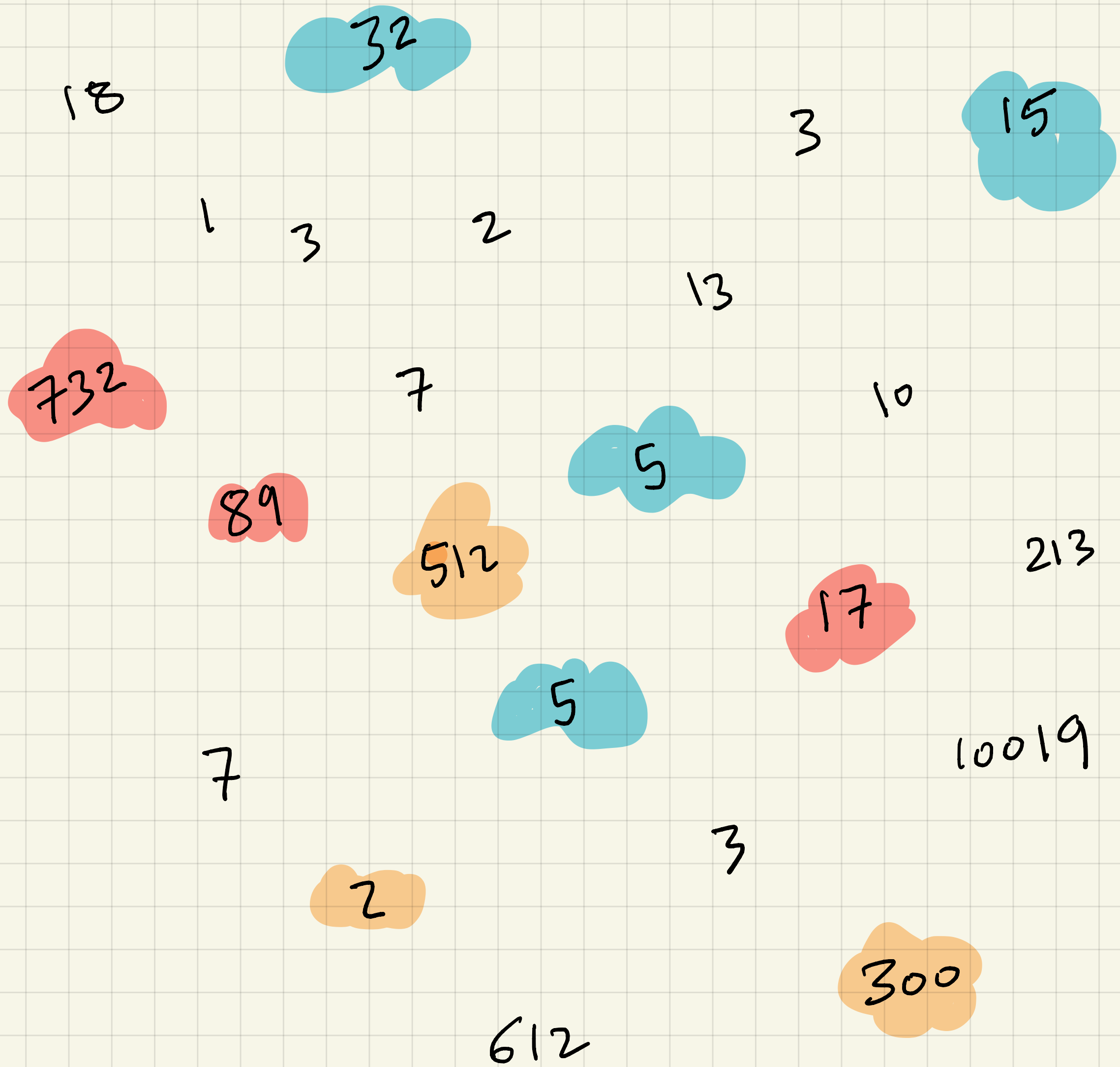

Some Number theory

Lecture 20

Number Theory

We focus on the positive integers.

Divisibility: Definition & Notation

1. a divides b e.g. 6 divides 18

2. a is a divisor of b

3. b is a multiple of a e.g 18 is multiple of 6

   $\exists\, m \in \mathbb{Z}.\ b = ma$ $18 = \underline{\underline{3}} \cdot 6$

4. $a \mid b$ (notation)

If a does NOT divide b, we can write $a \nmid b$.

We can always write (uniquely)

$$b = aq + r$$

where $0 \leq r < a$

q: quotient

r: remainder, $r \in \{0, 1, 2, \dots, a-1\}$ $(r = 0 \Longleftrightarrow a \mid b)$

Proof of uniqueness:

Suppose $b = aq_1 + r_1 \Rightarrow r_1 = b - aq_1$

$b = aq_2 + r_2 \Rightarrow r_2 = b - aq_2$

$q_1 \neq q_2$ and $r_1 > r_2$. Then $r_1 - r_2 = (b - aq_1) - (b - aq_2)$

so $r_1 - r_2 = a(q_2 - q_1)$

Since $0 \leq r_1 - r_2 < a$, then $0 \leq q_2 - q_1 < 1$, contradiction.

One interesting notion is a <u>common divisor</u>

d is common divisor of a and b

$$d \mid a \wedge d \mid b$$

$6 \mid 30$

$6 \mid 18$

Given $b = aq + r \quad (0 \leq r < a)$

$30 = 18(1) + \underbrace{12}_{r}$

$$d \mid a \wedge d \mid b \iff d \mid a \text{ and } d \mid r$$

$6 \mid 12$

Proof: • $d \mid a \wedge d \mid b \Rightarrow b = md \wedge a = nd \Rightarrow$

$$r = b - aq = md - ndq = d(m - nq) = dm'$$

so $d \mid r$.

• $d \mid a \wedge d \mid r \Rightarrow a = md \wedge r = nd \Rightarrow$

$$b = aq + r = mdq + nd = d(mq + n) = dm'$$

so $d \mid b$

This idea is behind one of the earliest algorithms in History, The Greatest Common Divisor algorithm due to Euclid.

First, observe that the greatest common divisor is a well defined concept (why)? :

1) Any two integers share at least one divisor : 1

2) A divisor of a number x, cannot be greater than x.

So the greatest common divisor exists.

Example: 300 and 18

Divisors of 300:

$\{1, 2, 3, 4, 5, 6, 10, 12, 15, 20, 25, 30, 50, 60, 75, 100, 150, 300\}$

Divisors of 18

$\{1, 2, 3, 6, 9, 18\}$

$$\gcd(300, 18) = 6$$

Not a practical approach!

Too much time to find all divisors.

Another idea: Factoring into primes

$$300 = 2^2 \cdot 3 \cdot 5^2$$

$$18 = 2 \cdot 3^2 \cdot 5^0$$

For each prime factor, pick the smaller power:

$$\gcd(300, 18) = 2^1 \cdot 3^1 \cdot 5^0 = 6$$

Side remark: What happens if we pick for each prime factor the largest power?

$$2^2 \cdot 3^2 \cdot 5^2 = 900$$

This is the least common multiple lcm.

Observation: $\gcd(a,b) \times \mathrm{lcm}(a,b) = a \times b$.

Also not a practical approach: Factoring into primes not easy!

Euclid's algorithm:

Construct a sequence

$$\underbrace{a_0 \quad a_1}_{300 \quad 18} \quad a_2 \quad \dots \quad a_{i-2} \quad a_{i-1} \quad a_i \quad \dots \quad a_k \quad \underbrace{a_{k+1}}_{0}$$

where $a_{i-2} = a_{i-1} q_{i-1} + \underbrace{a_i}_{\text{remainder of } a_{i-2}/a_{i-1}}$

Then $a_k = \gcd(a_0, a_1)$

Example:

	a_0	a_1	a_2	a_3	a_4
	300	18	12	6	0

$300 = 18(16) + \underbrace{12}_{\text{remainder}}$

$\gcd(300, 18) = \gcd(18, 12) = \gcd(12, 6)$

since $6 \mid 12$

100 39 22 17 5 2 1 0

$$\begin{array}{r|l} 100 & 39 \\ 78 & 2 \\ \hline 22 & \end{array} \qquad \begin{array}{r|l} 39 & 22 \\ 22 & 1 \\ \hline 17 & \end{array}$$

Do Long division.

$$\begin{array}{r|l} 22 & 17 \\ 17 & 1 \\ \hline 5 & \end{array} \qquad \begin{array}{r|l} 17 & 5 \\ 15 & 3 \\ \hline 2 & \end{array}$$

$$\begin{array}{r|l} 5 & 2 \\ 4 & 2 \\ \hline 1 & \end{array} \qquad \begin{array}{r|l} 2 & 1 \\ 2 & 2 \\ \hline 0 & \end{array}$$

Why is this good? It's efficient (Fast)

$a_0 \quad a_1 \quad a_2 \quad \cdots \quad a_{i-2} \quad a_{i-1} \quad a_i \quad \cdots \quad a_k \quad \underbrace{a_{k+1}}_{0}$ (decreasing)

where $a_{i-2} = a_{i-1} q_{i-1} + \underbrace{a_i}_{\text{remainder of } a_{i-2}/a_{i-1}}$

$$\boxed{\begin{aligned} a_{i-2} &\geqslant a_{i-1} + a_i \\ a_{k-1} &\geqslant 2 \\ a_k &\geqslant 1 \end{aligned}} \quad (q_{i-1} \geqslant 1) \qquad \text{V.S.} \qquad \boxed{\begin{aligned} F_n &= F_{n-1} + F_{n-2} \\ F_3 &= 2 \\ F_2 &= 1 \end{aligned}}$$

$$\begin{array}{ccccc} F_2 & F_3 & \cdots & F_{k+2} & (k+1 \text{ terms}) \\ \wedge\!\!\!| & \wedge\!\!\!| & & \wedge\!\!\!| & \\ a_k & a_{k-1} & \cdots & a_0 & \end{array}$$

$a_0 \geqslant F_{k+2} \approx \frac{1}{\sqrt{5}} \phi^{k+2} \Rightarrow k$ is logarithmic in a_0

The extended Euclidean alg.

$$a_0 \quad a_1 \quad a_2 \quad \cdots \quad a_{i-2} \quad a_{i-1} \quad a_i \quad \cdots \quad a_k \quad \underbrace{a_{k+1}}_{0}$$

First, a claim:

$$a_i = a_0 x_i + a_1 y_i \qquad x_i, y_i \in \mathbb{Z} \quad \text{(not unique)}$$

Every number in the sequence is a linear combination of a_0 and a_1

Example: $\underset{a_0}{\underline{300}}$ $\underset{a_1}{\underline{18}}$ 12 6 0

$$\begin{aligned}
300 &= a_0 \cdot 1 + a_1 \cdot 0 \\
18 &= a_0 \cdot 0 + a_1 \cdot 1 \\
12 &= a_0 \cdot 1 + a_1 (-16) \\
6 &= a_0 (-1) + a_1 \cdot 17 \\
0 &= a_0 (3) + a_1 (-50)
\end{aligned}$$

Euclidean alg. can find x_i and y_i

- Before we prove claim and find x_i, y_i, what's in this?
- Well, gcd is one integer in the sequence
- So we can write

$$\boxed{\gcd(a,b) = ar - bs} \qquad \underbrace{(r \geq 0,\ s \geq 0)}_{\text{how?}}$$

How: $\quad ar - bs = a(r+b) - b(s+a)$

- Why is this useful? (Later)

Proof that $a_i = a_0 x_i + a_1 y_i$ for all a_i is seq.

Base case:

$$a_0 = a_0 \cdot 1 + a_1 \cdot 0 \quad \checkmark$$

$$a_1 = a_0 \cdot 0 + a_1 \cdot 1 \quad \checkmark$$

Inductive hypothesis: Assume for a fixed $i \geq 1$,

$$a_j = a_0 x_j + a_1 y_j \quad \text{for all } 0 \leq j \leq i$$

Inductive hypothesis: Consider $i+1$

$$a_{i+1} = a_{i-1} - a_i q_i$$

$$= a_0 x_{i-1} + a_1 y_{i-1} - q_i (a_0 x_i + a_1 y_i)$$

$$= a_0 \underbrace{[x_{i-1} - q_i x_i]}_{x_{i+1}} + a_1 \underbrace{[y_i - q_i y_i]}_{y_{i+1}}$$

$$x_i = x_{i-2} - q_{i-1}\, x_{i-1}$$

$$y_i = y_{i-2} - q_{i-1}\, y_{i-1}$$

$$q_{i-1} = \frac{a_{i-2} - a_i}{a_{i-1}}$$

	a_0	a_1	$\cdots$	a_{i-2}	a_{i-1}	a_i	$\cdots$	$\gcd(a_0, a_1)$	0
x	1	0		x_{i-2}	x_{i-1}	?			
y	0	1		y_{i-2}	y_{i-1}	?			

Example:

300	18	12	6	0
1	0	1	-1	3
0	1	-16	17	-50

$$
\begin{aligned}
\gcd(300, 18) &= 300(-1) + 18(17) \\
&= 300(-1) - 18(-17) \\
&= 300(-1+18) - 18(-17+300) \\
&= 300\underbrace{(17)}_{\geq 0} - 18\underbrace{(283)}_{\geq 0}
\end{aligned}
$$